UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/698,507	10/26/2000	Rolf E. Carlson	xRCa-12	3367

			EXAMINER
20995	7590	05/19/2006	HOFFMAN, BRANDON S

KNOBBE MARTENS OLSON & BEAR LLP
2040 MAIN STREET
FOURTEENTH FLOOR
IRVINE, CA 92614

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 05/19/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.	Applicant(s)
Office Action Summary	09/698,507	CARLSON, ROLF E.
	Examiner	Art Unit
	Brandon S. Hoffman	2136

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>06 March 2006</u>.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final. .

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-70</u> is/are pending in the application.

   4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1-70</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

   Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

   Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   a)☐ All b)☐ Some * c)☐ None of:

   1.☐ Certified copies of the priority documents have been received.

   2.☐ Certified copies of the priority documents have been received in Application No. _____.

   3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

   * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☐ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date _____.

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____.

DETAILED ACTION

1.   Claims 1-70 are pending in this office action, claims 1, 16, 17, 24, 25, 36-38, 44,

49, 55, 58, and 68 are amended.

2.   Applicant's arguments, filed March 6, 2006, have been fully considered but they

are not persuasive.

Rejections

3.   The text of those sections of Title 35, U.S. Code not included in this action can

be found in a prior Office action.

Claim Rejections - 35 USC § 112

4.   The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly
> claiming the subject matter which the applicant regards as his invention.

5.   Claims 17-24 are rejected under 35 U.S.C. 112, second paragraph, as being

indefinite for failing to particularly point out and distinctly claim the subject matter which

applicant regards as the invention.

6.   Claim 17 recites the limitation "said remote machine" in the last limitations.

There is insufficient antecedent basis for this limitation in the claim.

7.   Claims 18-24 are dependent upon claim 17 and therefore inherit its deficiencies.

Claim Rejections - 35 USC § 103

8.   Claims 1-70 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Ramasubramani et al. (U.S. Patent No. 6,233,577) in view of Vuong et al. (U.S. Patent

No. 5,762,552).

        Regarding claims 1, 11-13, 17, and 47, Ramasubramani et al. teaches a casino

gaming system, comprising:

*   A plurality of gaming machines (fig. 3, ref. num 302);

*   A gaming server (fig. 3, ref. num 114) **said gaming server** comprising: a plurality

    of keys (fig. 3, ref. num 326), each of said plurality of keys including a time

    stamp, said time stamp indicating a period of time for which each of said plurality

    of keys is used (col. 10, lines 47-59); a random number generator that generates

    said plurality of keys; and an encryption algorithm (col. 10, line 60 through col.

    11, line 17),

*   A network bus interconnecting said plurality of gaming machines and said

    gaming server, said network bus used to transmit information between said

    plurality of gaming machines and said gaming server (fig. 3, ref. num 102),

*   Said gaming server transmitting said at least one of said plurality of keys over

    said network bus to at least one of said plurality of gaming machines where said

    key is decrypted (col. 4, lines 29-50),

- Said at least one of said plurality of gaming machines using said at least one of said plurality of keys to encrypt said information (fig. 1, step 5, client encrypts session key),

- Said at least one of said plurality of gaming machines transmitting said encrypted information over said network bus (fig. 1, step 5, client sends the encrypted session key over the network).

Ramasubramani et al. does not specifically teach the client and server to be a gaming machine and a gaming server, the gaming machine is **configured to determine an outcome of a game,** the gaming server is **configured to determine an outcome of a game and receive a request to initiate game play on a gaming machine from a remote machine**, or sending the information **to said remote machine**.

Vuong et al. teaches a gaming machine and a gaming server (fig. 1, ref. num 14 and 16), the gaming machine is **configured to determine an outcome of a game** (col. 6, lines 49-52), the gaming server is **configured to determine an outcome of a game and receive a request to initiate game play on a gaming machine from a remote machine** (fig. 8A and col. 14, lines 36-65), and sending the information **to said remote machine** (col. 14, lines 50-53).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine using a gaming machine and a gaming server, as taught by Vuong et al., with the system of Ramasubramani et al. It would have been obvious for such modifications because gambling provides a euphoric feeling to users, with the added benefit of being able to play at home.

Regarding claim 25, Ramasubramani et al. teaches a method for communicating information using a casino gaming system having at least one gaming machine and a gaming server, said method comprising:

- Establishing a first communication link between said at least one gaming machine and said gaming sever (fig. 1, step 1, client initiates a connection);

- First transmitting at least one of a plurality of keys stored at said gaming server over said first communication link from said gaming server to said at least one gaming machine (col. 4, lines 29-50);

- Encrypting information sent from said at least one gaming machine using said at least one of said plurality keys (fig. 1, step 5, client encrypts session key);

- Second transmitting said encrypted information over said first communication link from said at least one gaming machine (fig. 1, step 5, client sends the encrypted session key over the network); and

- Decrypting said received encrypted information **using said at least one of said plurality of keys** (col. 5, lines 27-47).

Ramasubramani et al. does not specifically teach the client and server to be a gaming machine and a gaming server, **receiving a request on said gaming server from a remote machine to initiate game play on said at least one gaming machine, determining an outcome of said game play on said at least one gaming machine, receiving encrypted information from said remote machine** and transmitting the information **to said remote machine**

Vuong et al. teaches a gaming machine and a gaming server (fig. 1, ref. num 14 and 16), **receiving a request on said gaming server from a remote machine to initiate game play on said at least one gaming machine** (fig. 8A and col. 14, lines 36-65), **determining an outcome of said game play on said at least one gaming machine** (col. 6, lines 49-52), **receiving encrypted information from said remote machine** and transmitting the information **to said remote machine** (col. 14, lines 50-53).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine using a gaming machine and a gaming server, as taught by Vuong et al., with the system of Ramasubramani et al. It would have been obvious for such modifications because gambling provides a euphoric feeling to users, with the added benefit of being able to play at home.

Regarding <u>claim 38</u>, <u>Ramasubramani et al.</u> teaches a casino gaming system for communicating information using asymmetric key pairs that includes a private key and a public key, said casino gaming system comprising:

- A plurality of gaming machines (fig. 3, ref. num 302);

- A certificate authority server including a memory storing at least a plurality of said public keys of said asymmetric key pairs (fig. 3, ref. num 114 and 326);

- A network bus interconnecting said plurality of gaming machines and said certificate authority server (fig. 3, ref. num 102),

- Said certificate authority server transmitting at least one of said plurality of public keys over said network bus to at least one of said plurality of gaming machines wherein said certificate authority server signs said at least one of said plurality of public keys transmitted over said network bus (col. 4, lines 29-50),

- Said at least one of said plurality of gaming machines using said at least one of said plurality of said public keys to encrypt information (fig. 1, step 5, client encrypts session key),

- Said at least one of said plurality of gaming machines transmitting said encrypted information over said network bus **to said remote machine** (fig. 1, step 5, client sends the encrypted session key over the network).

<u>Ramasubramani et al.</u> does not specifically teach the client and server to be a gaming machine and a gaming server, or **each configured to determine an outcome of a game of game play and provide said outcome to a remote machine**

Vuong et al. teaches a gaming machine and a gaming server (fig. 1, ref. num 14

and 16), and **each configured to determine an outcome of a game of game play**

and provide said outcome to a remote machine (col. 6, lines 49-52 and col. 14, lines

50-53).

It would have been obvious to one of ordinary skill in the art, at the time the

invention was made, to combine using a gaming machine and a gaming server, as

taught by Vuong et al., with the system of Ramasubramani et al. It would have been

obvious for such modifications because gambling provides a euphoric feeling to users,

with the added benefit of being able to play at home.

Regarding claims 49 and 55-57, Ramasubramani et al. teaches a casino gaming

system connected to at least one outside computer via an outside network, said casino

gaming system comprising:

- A gaming server (fig. 3, ref. num 114);

- A plurality of gaming machines located in a casino (fig. 3, ref. num 302),

- **Wherein said gaming server is configured to provide at least one**

  encryption key to said at least one of the gaming machines (col. 4, lines 29-

  50);

- A network bus connected to said gaming server and each of said plurality of

  access switches (fig. 3, ref. num 102);

- Said outside network connected to said gaming server (fig. 3, ref. num 102

  connected to 114).

Ramasubramani et al. does not teach a plurality of access switches, connecting

the gaming machine to the access switch when said one of said plurality of gaming

machines is idle, or one of said plurality of access switches connecting one of said

plurality of gaming machines and said outside computer over said outside network, the

gaming machines are **configured to determine an outcome of a game, wherein said**

gaming server is configured to receive a request to initiate game play on at least

one of the gaming machines from said at least one outside computer and wherein

said at least one of the gaming machines is configured to use said at least one

encryption key to communicate with said at least one outside computer

Vuong et al. teaches a plurality of access switches, each one of said plurality of

access switches individually connected to a different one of said plurality of gaming

machines; connecting the gaming machine to the access switch when said one of said

plurality of gaming machines is idle; and one of said plurality of access switches

connecting one of said plurality of gaming machines and said outside computer over

said outside network, so as to enable a remote player of said outside computer to play

said one of said plurality of gaming machines (fig. 8A and col. 13, line 63 through col.

14, line 14), **the other of said plurality of access switches disconnecting said**

outside computer from the other of said plurality of gaming machines (fig. 8A, ref.

num 120), the gaming machines are **configured to determine an outcome of a game**

(col. 6, lines 49-52), **wherein said gaming server is configured to receive a request**

to initiate game play on at least one of the gaming machines from said at least

one outside computer (fig. 8A and col. 14, lines 36-65) **and wherein said at least**

one of the gaming machines is configured to use said at least one encryption key

to communicate with said at least one outside computer (col. 14, lines 50-53).

It would have been obvious to one of ordinary skill in the art, at the time the

invention was made, to combine connecting the gaming machine to the access switch

when said one of said plurality of gaming machines is idle, as taught by <u>Vuong et al.</u>,

with the system of <u>Ramasubramani et al.</u> It would have been obvious for such

modifications because selecting an idle machine prevents errors from occurring on a

machine that is being simultaneously used by two different people.

Regarding <u>claims 58, 68, and 70</u>, <u>Ramasubramani et al.</u> teaches a method for

communicating with a plurality of gaming machines in a casino, said plurality of gaming

machines connected to a gaming server, said method comprising the steps of:

- Providing **an encryption key to said identified one of said plurality of gaming**

  machines (col. 4, lines 29-50);

- Enabling the remote player to play a casino game at said identified one of said

  plurality of gaming machines (fig. 1, step 6, a secure connection is created).

Ramasubramani et al. does not teach receiving a request from an outside

network for an identified one of said plurality of gaming machines, or delivering to said

outside network a gaming machine unavailable message when said identified one of

said plurality of gaming machines is in use, **determining the outcome of a game on**

said identified one of said plurality of gaming machines or **transmitting data**

encrypted using said encryption key from said identified one of said plurality of

gaming machines over a secured communication link between said outside network

and said identified one of said plurality of gaming machines.

Vuong et al. teaches receiving a request from an outside network for an identified

one of said plurality of gaming machines, said request initiated by a remote player; and

waiting for an idle gaming machine and delivering to said outside network a gaming

machine unavailable message when said identified one of said plurality of gaming

machines is in use (fig. 8A and col. 13, lines 63 through col. 14, line 14), **determining**

the outcome of a game on said identified one of said plurality of gaming

machines (col. 6, lines 49-52); and **transmitting data encrypted using said**

encryption key from said identified one of said plurality of gaming machines over

a secured communication link between said outside network and said identified one of

said plurality of gaming machines (col. 14, lines 50-53).

It would have been obvious to one of ordinary skill in the art, at the time the

invention was made, to combine waiting for an idle gaming machine and delivering to

said outside network a gaming machine unavailable message when said identified one

of said plurality of gaming machines is in use, as taught by Vuong et al., with the system

of Ramasubramani et al. It would have been obvious for such modifications because

waiting for a machine to be idle prevents errors from occurring on a machine that is

being simultaneously used by two different people.

Regarding claims 2-5, 18, 19, 26, 27, and 54, the examiner takes Official notice

that said plurality of keys are symmetric session keys, wherein the keys use DES or

triple-DES algorithms. It would have been obvious to use symmetric session keys

because symmetric keys are faster.

Regarding claims 6, 20, 28, and 53, Ramasubramani et al. as modified by Vuong

et al. teaches wherein said plurality of keys comprise asymmetric key pairs (see col. 3,

line 60 through col. 4, line 8 of Ramasubramani et al.).

Regarding claims 7, 21, and 29, Ramasubramani et al. as modified by Vuong et

al. teaches wherein said asymmetric keys are session keys (see col. 3, lines 48-59 of

Ramasubramani et al.).

Regarding claim 8, Ramasubramani et al. as modified by Vuong et al. teaches

wherein said asymmetric key pairs comprise Rivest, Shamir, and Adleman (RSA)

algorithms (see col. 4, lines 3-8 of Ramasubramani et al.).

Regarding claims 9, 30, and 40, Ramasubramani et al. as modified by Vuong et al. as modified by Vuong et al. teaches wherein said gaming server is interconnected to an outside network (see col. 4, lines 52-66 of Ramasubramani et al.).

Regarding claims 10, 31, 41, 50, and 67, Ramasubramani et al. as modified by Vuong et al. teaches wherein said outside network is the Internet (see col. 4, lines 52-66 of Ramasubramani et al.).

Regarding claims 32 and 46, Ramasubramani et al. as modified by Vuong et al. teaches wherein said gaming server further comprises a random number generator that generates said plurality of keys (see col. 10, line 60 through col. 11, line 17 of Ramasubramani et al.).

Regarding claims 14, 22, and 42, Ramasubramani et al. as modified by Vuong et al. teaches wherein said encrypted information is transmitted over said network bus to another of said at least one gaming machines (see fig. 2, ref. num 104 and 110 of Ramasubramani et al.).

Regarding claims 15, 23, and 43, Ramasubramani et al. as modified by Vuong et al. teaches wherein said encrypted information is transmitted over said network bus to said gaming server (see fig. 1, step 5 of Ramasubramani et al., client sends the encrypted session key over the network).

Regarding claims 16, 24, and 44, Ramasubramani et al. as modified by Vuong et al. teaches further comprising:

- An outside network connected to said gaming server (see fig. 2, ref. num 104 of Ramasubramani et al.); and

- A remote **machine** connected to said outside network wherein said encrypted information is transmitted over said network bus and said outside network to said remote **machine** (see fig. 2, ref. num 110 of Ramasubramani et al.).

Regarding claim 33, Ramasubramani et al. as modified by Vuong et al. teaches further comprising the steps of encrypting each of said plurality of keys transmitted from said gaming server to said at least one gaming machine (see col. 5, lines 41-47 of Ramasubramani et al.).

Regarding claim 34, Ramasubramani et al. as modified by Vuong et al. teaches wherein said step of second transmitting further comprises transmitting said encrypted information over said first communication link to another of said at least one gaming machine (see fig. 2, ref. num 104 and 110 of Ramasubramani et al.), and wherein said step of decrypting further comprises decrypting said received encrypted information at said another of said at least one gaming machine (see col. 5, lines 27-47 and col. 9, lines 8-47 of Ramasubramani et al.).

Regarding claim 35, Ramasubramani et al. as modified by Vuong et al. teaches wherein said step of transmitting further comprises second transmitting said encrypted information over said first communication link to said gaming server, and wherein said step of decrypting further comprises decrypting said received encrypted information at said gaming server (see col. 5, lines 39-47 of Ramasubramani et al.).

Regarding claim 36, Ramasubramani et al. as modified by Vuong et al. teaches further comprising the step of establishing a second communication link between said gaming server and a remote **machine** (see fig. 2, connection between 114 and 110 of Ramasubramani et al.).

Regarding claim 37, Ramasubramani et al. as modified by Vuong et al. teaches wherein said step of transmitting further comprises transmitting said encrypted information over said first communication link and said second communication link to said remote **machine**, and wherein said step of decrypting further comprises decrypting said received encrypted information at said remote **machine** (see col. 9, lines 8-47 of Ramasubramani et al.).

Regarding claim 39, Ramasubramani et al. as modified by Vuong et al. teaches wherein each of said plurality of gaming machines validates said at least one of said signed plurality of public keys received from said network bus (see col. 3, lines 57-59 of Ramasubramani et al.).

Regarding claim 45, Ramasubramani et al. as modified by Vuong et al. teaches wherein said network bus is connected to at least one gaming server, said certificate authority server transmitting at least one of said plurality of said public keys to said at least one gaming server, said gaming server encrypts information using said at least one of said plurality of said public keys, said gaming server transmits said encrypted information over said network bus (see col. 5, lines 41-47 of Ramasubramani et al.).

Regarding claim 48, Ramasubramani et al. as modified by Vuong et al. teaches wherein said network bus is connected to a plurality of other certificate authority servers (see fig. 4A, ref. num 356 and 358 of Ramasubramani et al.), said certificate authority server transmitting at least one of said plurality of said public keys to said plurality of other certificate authority servers wherein said plurality of other certificate authority servers encrypts information using said at least one of said plurality of said public keys and transmits said encrypted information over said network bus (see col. 4, lines 29-41 of Ramasubramani et al.).

Regarding claim 51, the combination of Ramasubramani et al. in view of Vuong et al. teaches further comprising a certificate authority server connected to said network bus, said certificate authority server including a plurality of public keys of a plurality of asymmetric key pairs (see fig. 3, ref. num 124 of Ramasubramani et al.).

Regarding claim 52, the combination of Ramasubramani et al. in view of Vuong

et al. teaches wherein said outside computer acquires one of said plurality of public

keys from said certificate authority server via said outside network and said network

bus, said outside computer using said one of said plurality of public keys to encrypt

information transmitted to said one of said plurality of gaming machines over said

outside network and said network bus (see fig. 1, step 5 of Ramasubramani et al.).

Regarding claim 59, the combination of Ramasubramani et al. in view of Vuong

et al. teaches wherein said step of receiving a request further comprising the steps of

entering player identification information; and providing said entered player identification

information to a database (see fig. 4, ref. num 74 of Vuong et al.).

Regarding claim 60, the combination of Ramasubramani et al. in view of Vuong

et al. teaches wherein said step of providing said entered player identification

information further comprises the steps of:

- Comparing said entered player identification information to said database (see

   col. 7, lines 10-32 of Ramasubramani et al.); and

- Providing said secured communication link between said outside network and

   said identified one of said plurality of gaming machines if said entered

   identification information matches an entry in said database (see col. 7, lines 10-

   32 of Ramasubramani et al.).

Regarding claim 61, the combination of Ramasubramani et al. in view of Vuong

et al. teaches wherein said entered player identification information is credit card

information (see col. 2, lines 43-59 of Vuong et al.).

Regarding claim 62, the combination of Ramasubramani et al. in view of Vuong

et al. teaches further comprising the steps of documenting information about the remote

player (see col. 8, lines 7-27 of Vuong et al.).

Regarding claim 63, the combination of Ramasubramani et al. in view of Vuong

et al. teaches wherein said documented information comprises information about the

remote player (see col. 8, lines 7-27 of Vuong et al.).

Regarding claim 64, the combination of Ramasubramani et al. in view of Vuong

et al. teaches wherein said documented information comprises a time for which the

remote player plays said one of said plurality of gaming machines (see col. 8, lines 7-27

of Vuong et al.).

Regarding claim 65, the combination of Ramasubramani et al. in view of Vuong

et al. teaches wherein said documented information comprises a location from which

the remote player is playing (see col. 8, lines 62-66 of Vuong et al.).

Regarding claim 66, the combination of Ramasubramani et al. in view of Vuong

et al. teaches wherein said documented information comprises an amount the remote

player has wagered (see col. 8, lines 62-66 of Vuong et al.).

Regarding claim 69, the combination of Ramasubramani et al. in view of Vuong

et al. teaches wherein said plurality of gaming machines are located in a casino (see fig.

1 of Vuong et al.).

Response to Arguments

9.   Applicant's arguments have been considered but are moot in view of the new

ground(s) of rejection.

Conclusion

10.   Applicant's amendment necessitated the new ground(s) of rejection presented in

this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP

§ 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37

CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later

than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Brandon S. Hoffman whose telephone number is 571-

272-3863. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number

for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free).

BH

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100